

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)(1) a Gray Apple iPhone 12 Pro Max and (2) a Black
Apple iPhone 8 Plus**23 MAG 7151**

Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

18 USC §§ 371, 666, 1343, and 1349, and 52 U.S.C. § 30121

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment A

YOU ARE COMMANDED to execute this warrant on or before November 22, 2023 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

11/09/2023 at 2:17 p.m.

City and state:

New York, New York


Judge's signature

Hon. Sarah Netburn, U.S.M.J.

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

Attachment A

I. The Subject Devices

The Subject Devices are particularly described as: (1) a grey Apple iPhone 12 Pro MAX with serial number F2LDQ5LM0D47 (“Subject Device-1”) and (2) a black Apple iPhone 8 Plus with serial number FD1Y54XBJCM2 (“Subject Device-2”). This warrant authorizes the extraction of data from the Subject Devices and the review of any data extracted from the Subject Devices.

II. Seizure and Review of ESI on the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”) described as follows:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Devices.
2. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign of Eric Adams (the “Adams Campaign”) on the part of [REDACTED] and its employees, officers, or associates ([REDACTED] the Turkish Government, including its Consulate General in New York and its employees, officers, or associates; or the Adams Campaign.
3. Evidence relating to coordination between [REDACTED] Turkish nationals, or the Turkish Government and the Adams Campaign concerning political contributions to the Adams Campaign, including, but not limited to, evidence of motive and intent for [REDACTED] Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaign to provide benefits, whether lawfully or unlawfully, to [REDACTED] Turkish nationals, or the Turkish Government in return for campaign contributions.
4. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaign.
5. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaign originating from Turkish nationals.

2022.01.31

6. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

7. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

8. Evidence of the relationship between and among (i) [REDACTED] (ii) the Turkish Government, or (iii) Turkish nationals covertly contributing to the Adams Campaign, and any person who is or was associated with or employed by the Adams Campaign, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

9. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by the Adams Campaign, including but not limited to straw donations and any actions taken by any person who is or was associated with or employed by the Adams Campaign on behalf of the Turkish Government, [REDACTED] or entities and persons acting at the behest of the Turkish Government.

10. Evidence regarding any requests by the Adams Campaign for matching funds based on donations from [REDACTED] personnel, or any other straw donors, including any discussions of matching funds.

11. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Subject Devices.

12. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

13. Evidence concerning efforts to destroy evidence of the Subject Offenses or to devise or coordinate false exculpatory explanations for the conduct underlying the Subject Offenses.

B. Review of ESI

Following seizure of any electronic communications devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the device was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

UNITED STATES DISTRICT COURT

for the

_____ District of _____

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

Case No. **23 MAG 7151**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

The application is based on these facts:

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s authorized electronic signature

Applicant's signature

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
(specify reliable electronic means).

Date: _____

City and state: _____

Judge's signature

Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for (1) a Gray Apple iPhone 12 Pro Max and (2) a Black Apple iPhone 8 Plus

23 MAG 7151
TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

██████████ being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since 2019. I am currently assigned to a public corruption squad of the New York Field Office, where, among other things, I investigate crimes involving illegal campaign contributions, theft of federal funds, and bribery. Through my training and experience, I also have become familiar with some of the ways in which individuals use smart phones and electronic communications, including social media, email, and electronic messages, in furtherance of their crimes, and have participated in the execution of search warrants involving electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the “Subject Devices”) for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during

the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Devices

3. The Subject Devices are particularly described as: (1) a grey Apple iPhone 12 Pro MAX with serial number F2LDQ5LM0D47 (“Subject Device-1”) and (2) a black Apple iPhone 8 Plus with serial number FD1Y54XBJCM2 (“Subject Device-2”).

4. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs.

5. The Subject Devices are presently located in the office of the FBI located in the Southern District of New York.

C. The Subject Offenses

6. For the reasons detailed below, I respectfully submit that there is probable cause to believe that the Subject Devices contain evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”).

II. Probable Cause

A. Probable Cause Regarding Subjects’ Commission of the Subject Offenses

7. On November 5, 2023, the Honorable Gary Stein, United States Magistrate Judge for the Southern District of New York, issued a warrant authorizing a search of the person and personal effects of Eric Adams and the seizure of any electronic communications devices found in

that search. The search warrant (the “Adams Phone Warrant”), and the application for that warrant, including the affidavit in support and its exhibits (the application and its exhibits are collectively referred to as the “Adams Phone Warrant Application”), are attached as Exhibit A and incorporated by reference herein.¹ As set forth in the Adams Phone Warrant Application, Adams used a cellphone with the call number [REDACTED] 3179 (the “Adams Personal Cellphone”), and a number of Adams’s communications about the Subject Offenses were conducted using the Adams Personal Cellphone. (*See generally* Ex. A ¶ 15).

B. Probable Cause Justifying Search of the Subject Devices

8. In the evening on November 6, 2023, I and other FBI Special Agents executed the Adams Phone Warrant, as Adams was leaving an event held near Washington Square Park in Manhattan. During the execution of the Adams Phone Warrant, Adams handed over four electronic devices, two of which were cellphones.

9. However, based on my discussions with other law enforcement personnel, I know that neither of the cellphones seized in the execution of the Adams Phone Warrant were associated with the call number of the Adams Personal Cellphone.

10. From my involvement in this investigation, I know that on or about November 7, 2023, in response to a subpoena, Adams’s counsel brought two electronic devices—the Subject Devices—to the FBI’s offices in Manhattan. I understand that Adams’s counsel has asserted, in substance and in part, that the Subject Devices were both, at different times, associated with the

¹ On November 6, 2023, the Honorable Sarah Netburn, United States Magistrate Judge for the Southern District of New York, issued a second search warrant that was the same as the Adams Phone Warrant, except that it authorized execution outside of the Southern District of New York pursuant to Fed. R. Crim. P. 41(b)(2). Because Adams was found within the Southern District of New York, law enforcement did not execute that second search warrant.

call number of the Adams Personal Cellphone, and that they were not in Adams's possession at the time of the search warrant execution discussed above.

11. Also from my involvement in the investigation, I further understand that Adams's counsel indicated, in substance and in part, that the Subject Devices should be imaged by the FBI and returned as promptly as possible. Additionally, I understand that Adams's counsel provided the FBI with the passcode for Subject Device-2, but represented that Adams had accidentally locked Subject Device-1 and could not remember the passcode for Subject Device-1. Upon receiving the Subject Devices, the FBI began imaging Subject Device-2, for which Adams's counsel provided a password. Because Adams has not been asked to sign and has not signed a written consent to search the Subject Devices, however, the FBI has not yet reviewed the contents of the Subject Devices. I am now seeking a warrant to search the Subject Devices, and in particular to review any data that the FBI is able to extract from the Subject Devices, prior to reviewing any data extracted from the Subject Devices.

12. As explained in the Adams Phone Warrant Application that is attached to this affidavit and incorporated by reference herein, I respectfully submit there is probable cause to believe that the subjects of the investigation described therein committed the Subject Offenses, that Adams used one or more devices associated with the call number of the Subject Devices to exchange communications relevant to the Subject Offenses, and that the evidence, fruits, and instrumentalities of the Subject Offenses listed in Attachment A, which is incorporated by reference herein, will be found on the Subject Devices.

III. Procedures for Searching ESI

A. Review of ESI

13. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel

assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

14. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

15. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

B. Return of the Subject Devices

16. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject


Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

17. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.


18. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

/s authorized electronic signature


Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, on

November 9, 2023


HON. SARAH NETBURN
UNITED STATES MAGISTRATE JUDGE

Attachment A

I. The Subject Devices

The Subject Devices are particularly described as: (1) a grey Apple iPhone 12 Pro MAX with serial number F2LDQ5LM0D47 (“Subject Device-1”) and (2) a black Apple iPhone 8 Plus with serial number FD1Y54XBJCM2 (“Subject Device-2”). This warrant authorizes the extraction of data from the Subject Devices and the review of any data extracted from the Subject Devices.

II. Seizure and Review of ESI on the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”) described as follows:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Devices.

2. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign of Eric Adams (the “Adams Campaign”) on the part of [REDACTED] and its employees, officers, or associates ([REDACTED] the Turkish Government, including its Consulate General in New York and its employees, officers, or associates; or the Adams Campaign.

3. Evidence relating to coordination between [REDACTED] Turkish nationals, or the Turkish Government and the Adams Campaign concerning political contributions to the Adams Campaign, including, but not limited to, evidence of motive and intent for [REDACTED] Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaign to provide benefits, whether lawfully or unlawfully, to [REDACTED] Turkish nationals, or the Turkish Government in return for campaign contributions.

4. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaign.

5. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaign originating from Turkish nationals.

2022.01.31

6. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

7. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

8. Evidence of the relationship between and among (i) [REDACTED] (ii) the Turkish Government, or (iii) Turkish nationals covertly contributing to the Adams Campaign, and any person who is or was associated with or employed by the Adams Campaign, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

9. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by the Adams Campaign, including but not limited to straw donations and any actions taken by any person who is or was associated with or employed by the Adams Campaign on behalf of the Turkish Government, [REDACTED] or entities and persons acting at the behest of the Turkish Government.

10. Evidence regarding any requests by the Adams Campaign for matching funds based on donations from [REDACTED] personnel, or any other straw donors, including any discussions of matching funds.

11. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Subject Devices.

12. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

13. Evidence concerning efforts to destroy evidence of the Subject Offenses or to devise or coordinate false exculpatory explanations for the conduct underlying the Subject Offenses.

B. Review of ESI

Following seizure of any electronic communications devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the device was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

Exhibit A
[23 MAG 7090]